UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
v.	)	Criminal Action No. 16-10010-PBS
JOHN TRAN,	)	
Defendant.	)	

MEMORANDUM AND ORDER

December 23, 2016

Saris, C.J.

INTRODUCTION

Defendant John Tran is charged with one count of possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B) and one count of receipt of child pornography in violation of 18 U.S.C. § 2252A(a)(2)(A).

This case -- like dozens of others currently pending across the country -- arises from an FBI investigation into users of Playpen, a child pornography website. Playpen operates on the Tor network, which enables anonymous internet browsing. In February 2015, the government acquired control of Playpen's server. For two weeks, the government operated the website. To obtain the IP addresses of the site's users, the government applied for and received a search warrant from a magistrate

judge in the Eastern District of Virginia. The search warrant allowed the FBI to deploy a Network Investigative Technique ("NIT") on users' computers around the country. The NIT caused users' computers to transmit identifying information, including IP addresses, to the government.

The defendant moves to dismiss the indictment on the basis that the government acted outrageously in maintaining the child pornography website Playpen for two weeks during the FBI's investigation. The defendant also moves to suppress all evidence gathered by the NIT as well as all fruits of the allegedly unconstitutional search.

For the reasons set forth below, the defendant's motion to dismiss (Docket No. 44) and motion to suppress (Docket No. 45) are **DENIED**.

FACTUAL BACKGROUND

The Court has previously described the facts of the FBI's Playpen investigation. See United States v. Anzalone ("Anzalone II"), No. 15-10347-PBS, 2016 WL 6476939, at *1-3 (D. Mass. Oct. 28, 2016) (denying defendant's motion to dismiss); United States v. Anzalone ("Anzalone I"), No. CR 15-10347-PBS, 2016 WL 5339723, at *1-5 (D. Mass. Sept. 22, 2016) (denying defendant's motion to suppress). The Court incorporates and assumes familiarity with these two opinions. The Court offers a brief review of those facts for the convenience of the reader.

I. The Tor Network

The Tor network, also known as The Onion Router, is an anonymity network that masks a user's IP address. To access the Tor network, a user must download an add-on to the user's existing browser or download the Tor browser bundle. To ensure anonymity for its users, the Tor network bounces communications through various relay computers. When a user accesses a website, the IP address of the last computer in that chain is displayed, rather than the user's IP address.

Within the Tor network, sites can be designed as "hidden services." Hidden services allow websites and other servers to hide their location by replacing a traditional IP address with a Tor-based web address.

II. The Playpen Website

Playpen was a website dedicated largely to child pornography. Playpen operated on Tor as a hidden service. According to Special Agent Douglas Macfarlane's affidavit in support of the February 20, 2015 search warrant, a user could not inadvertently arrive at the Playpen site: "Tor hidden services are not indexed like websites on the traditional Internet. Accordingly, unlike on the traditional Internet, a user may not simply perform a Google search for the name of one of the websites on Tor to obtain and click on a link to the site." Macfarlane Aff. ¶ 10, Docket No. 61, Ex. 1. To learn

Playpen's unique Tor address, a user might communicate directly with others on Tor or he might consult another site that lists links to child pornography hidden service sites. Agent Macfarlane concluded that accessing Playpen "therefore requires numerous affirmative steps by the user, making it extremely unlikely that any user could simply stumble upon [Playpen] without understanding its purpose and content." Id.

Agent Macfarlane described Playpen's homepage as it appeared on February 18, 2015, two days before he signed the affidavit. At the top left corner of the page, the name Playpen was prominently displayed. On either side of the site name were images depicting partially clothed prepubescent girls with their legs spread apart. Below these images, the site stated: "No cross-board reposts, .7z preferred, encrypt filenames, include preview . . . ." Id. ¶ 12. Agent Macfarlane explained that "no cross-board reposts" was an instruction to users not to post material appearing on other sites. The ".7z preferred" statement referred to a method of compressing large files for distribution. At the top right corner, to the right of the site name, users could enter a username and password, and select a session length. A login button appeared to the right of those login fields.

Below the site name, the image of the two partially clothed girls, and the login fields was a textbox that read: "Warning!

Only registered members are allowed to access the section. Please login below or 'register an account' . . . with Playpen." Id. The "register an account" text was hyperlinked to the site's registration page. Another set of login fields appeared below this warning, asking users to enter their username, password, minutes to stay logged in, and whether they wanted to permanently remain logged in.

When a prospective user clicked the "register an account" hyperlink, the user saw a message from the forum operators. The message explained that the forum required new users to enter an email address and that the software "checks that what you enter looks approximately valid." Id. ¶ 13. However, the forum operators encouraged users to enter fake email addresses: we "do NOT want you to enter a real address, just something that matches the xxx@yyy.zzz pattern. No confirmation email will be sent. This board has been intentionally configured so that it WILL NOT SEND EMAIL, EVER." Id. The message further cautioned new users: "For your security you should not post information here that can be used to identify you." Id. The forum operators emphasized the site's focus on anonymity: "The website is not able to see your IP and can not collect or send any other form of information to your computer except what you expressly upload," explaining that only a text file with the user's username and password reside in the browser's cache. Id.

The defendant and the government agree that one aspect of the homepage changed between February 18, 2015, when Agent Macfarlane last visited the Playpen site, and February 20, 2015, when Agent Macfarlane submitted the search warrant application. On February 18, 2015, Agent Macfarlane visited the Playpen site. He confirmed that the site's content had not changed. However, on February 19, 2015, the day after Agent Macfarlane's last visit and the day before he submitted the search warrant application, the logo on Playpen's site was altered. Instead of two prepubescent, partially clothed girls with their legs spread, the site featured one young girl (age unclear) wearing a short dress and black stockings with her legs crossed. Therefore, the affidavit incorrectly described the homepage. Agent Macfarlane did not know of this change when he signed the affidavit on February 20, 2015.

After logging into Playpen with a username and password, visitors to the site had access to various forums, many of which contained child pornography. Most of Playpen's content was not hosted directly on the Playpen site; instead, Playpen operated primarily as a bulletin board on which users posted links to other websites from which child pornography could be downloaded along with preview images and the passwords needed to download and decrypt the illegal files.

Various features of the site allowed for the dissemination of child pornography: a private messaging function, an image hosting feature, a file hosting feature, and a chat feature.

III. The NIT and the FBI Investigation

On February 19, 2015, the FBI arrested Steven Chase -- Playpen's principal administrator -- and assumed control of Playpen, moving a copy of the site to a government server in the Eastern District of Virginia. From that location, the government operated the website for two weeks, from February 20 to March 4, 2015, in order to identify the IP addresses of Playpen users. After procuring a warrant from a magistrate judge in the Eastern District of Virginia, the government deployed the NIT on users' computers that caused those computers to transmit their IP address and other pieces of identifying information back to the government. Because Playpen resided on the Tor network, Agent Macfarlane explained that the NIT was necessary to identify the site's users because other methods typically used in criminal investigations "have been tried and have failed or reasonably appear to be unlikely to succeed if they are tried." Id. ¶ 31. After obtaining users' IP addresses, the FBI paired that information with the content the users accessed on the site. The government then sought additional warrants to physically search users' homes for child pornography.

During the two weeks that the government ran Playpen, the defendant was logged in for a total of one hour and 47 minutes. After learning this and the defendant's IP address, the government sought a warrant to search his parents' home in Waltham, Massachusetts.

During the two-week period that the government operated Playpen, links to child pornography remained mostly accessible to the site's visitors. The government catalogued many of the images and videos that were made available via these links.

At no point during this two-week window did the FBI post new images, videos, or links to child pornography. Nor did the FBI enhance the site, either in its content or functionality, beyond what predated the government takeover.

The government did restore the site's file hosting feature, which was briefly down at the time the FBI seized the site and had existed prior to the government's seizure. Upon takeover, the government disabled a section of the site called the Producer's Pen. The Producer's Pen encouraged members to produce and share new child pornography. An undercover FBI agent, posing as the site's administrator, posted a message stating that this section would be revived in the near future. The agent wrote the message to prevent users from suspecting the government investigation. The Producer's Pen section never actually reappeared on the site.

The FBI reviewed all site postings, including chat and private messages, to assess and mitigate any potential harm to children. As of October 2016, about forty-nine children had been identified or rescued from hands-on abuse as a result of the investigation.

The government held regular meetings to assess whether to continue to operate Playpen. On March 4, 2015, after running the site for two weeks, the government shut it down.

DISCUSSION

I. Motion to Dismiss

The defendant argues that this case should be dismissed, asserting that the FBI's decision to continue operating the Playpen site for two weeks constituted outrageous government conduct.

Every district court to consider this same argument has found it wanting. See, e.g., United States v. Owens, No. 16-CR-38-JPS, 2016 WL 7079617, at *5 (E.D. Wis. Dec. 5, 2016) ("Whether the government should have operated the Playpen website in the manner it did is an entirely different question that is not before the Court today. The Court is confident, however, that the government's actions in this matter were not so outrageous as to justify the dismissal of the indictment against Mr. Owens."); United States v. Allain, No. 15-CR-10251, 2016 WL 5660452, at *13 (D. Mass. Sept. 29, 2016) (Burroughs,

J.) ("Reasonable minds will no doubt differ on whether the government made the right choice here, but it is not the rare case in which any misconduct on the part of the government was sufficiently blatant, outrageous, or egregious to warrant the dismissal of the indictment.").

This Court has also previously considered and rejected this outrageous conduct argument. Anzalone II, 2016 WL 6476939, at *5. As with the defendant in Anzalone, the defendant here is effectively asking the Court to second-guess the FBI's investigative techniques. The defendant asserts that the FBI could have performed aspects of the operation differently and still achieved similar results. That may or may not be true. But the standard for dismissal requires much more than that. See United States v. Guzman, 282 F.3d 56, 59 (1st Cir. 2002) ("[T]he outrageous government misconduct doctrine is reserved for the most appalling and egregious situations.").

The Court pauses momentarily to respond to two arguments not previously addressed in its Anzalone II order.

First, when describing the content of the Playpen site during the two-week period that the government operated it, the defendant says that the site included a "How To" advice section. He asserts that this section provided "instructional information about sexual abuse of children and avoiding detection." Docket No. 44 at 8. Allegedly, "[n]ew postings were added to this

section throughout the time that the FBI was operating the site." Id.

The defendant provides no evidence to corroborate these assertions. At hearing, the Court asked the defendant to provide a supplemental filing with such evidence. He has not done so. In the absence of any evidence that this section remained on the site during the two weeks in question and without a clearer sense of what information this section contained, the Court cannot consider these unsubstantiated assertions.

Second, the defendant argues that the government violated a number of laws, particularly 18 U.S.C. § 3509(m), in operating Playpen. Section 3509 was enacted as part of the Adam Walsh Act in 2006. The cited subsection states: "In any criminal proceeding, any property or material that constitutes child pornography (as defined by section 2256 of this title) shall remain in the care, custody, and control of either the Government or the court." 18 U.S.C. § 3509(m) (1). In his brief, the defendant omits the "in any criminal proceeding" language. See Docket No. 44 at 15. The plain language indicates that this section does not govern the FBI's investigative techniques here. Its placement in the code in Chapter 223, which outlines criminal procedure requirements for witnesses and other evidence, belies the defendant's argument that § 3509(m) applies to the investigation at issue. Finally, the defendant does not

cite any authority for the proposition that a violation of this section for law enforcement purposes supports a finding of outrageous government conduct.

The Court **DENIES** the defendant's motion to dismiss.

II. Motion to Suppress

In his motion to suppress, the defendant raises five arguments not explicitly addressed in the Court's Anzalone I order: (1) the NIT warrant was expressly limited to searches in the Eastern District of Virginia; (2) the warrant violated the Federal Magistrates Act (in addition to Federal Rule of Criminal Procedure 41); (3) the Rule 41 violation was deliberate; (4) the warrant was not supported by probable cause; and (5) a Franks hearing is warranted because, the defendant argues, one of the agents involved in the Playpen investigation was aware that the warrant application incorrectly described the Playpen homepage.

A. NIT Warrant's Geographic Scope

The defendant argues that the warrant is expressly limited to searches of computers in the Eastern District of Virginia. The government does not respond to this argument.

In support of this interpretation, the defendant cites the warrant's first page, which begins: "An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Virginia." Docket No. 45, Ex. 2 at 2.

The warrant then states that the magistrate judge should "[i]dentify the person or describe the property to be searched and give its location." Id. What follows is a notation to "See Attachment A." Id. Attachment A explains that the NIT would be deployed on the government server in the Eastern District of Virginia, and that the NIT would obtain information from "activating computers." See id. at 3. The warrant did not limit the location of the "activating computers" to the Eastern District of Virginia. See id. ("This warrant authorizes the use of a network investigative technique ('NIT') to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computers described below."). The warrant explained that the "activating computers are those of any user or administrator who logs into the TARGET WEBSITE by entering a username and password." Id. Attachment B outlined the data that would be seized from these activating computers: "From any 'activating' computer described in Attachment A," the NIT warrant was to seize seven pieces of data including the computer's IP address. Id. at 4.

A complete, contextual reading of the warrant demonstrates, as other district courts have found, that the warrant was not geographically limited to activating computers in the Eastern District of Virginia. See United States v. Levin, No. CR 15-10271-WGY, 2016 WL 2596010, at *5 n.8 (D. Mass. May 5, 2016)

(Young, J.) ("That the cover page of the NIT Warrant application indicated that the property to be searched was located in the Eastern District of Virginia does not alter this conclusion."); United States v. Michaud, No. 3:15–cr–05351–RJB, 2016 WL 337263 at *4 (W.D. Wash. Jan. 28, 2016) ("Mr. Michaud's argument requires an overly narrow reading of the NIT Warrant that ignores the sum total of its content. While the NIT Warrant cover sheet does explicitly reference the Eastern District of Virginia, that reference should be viewed within context . . . .").

The Court finds that the warrant permitted the NIT to gather data from activating computers outside of the Eastern District of Virginia.

B. Violation of the Federal Magistrates Act

The defendant argues that the NIT warrant failed to comply with the Federal Magistrates Act. The government says that the Court's analysis of Rule 41 in Anzalone I applies to the Federal Magistrates Act.

The Federal Magistrates Act states that a "United States magistrate judge serving under this chapter shall have within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law . . . (1) all powers and duties conferred or imposed upon United States

commissioners by law or by the Rules of Criminal Procedure for the United States District Courts . . . .” 28 U.S.C. § 636(a)(1).

Whether the Federal Magistrates Act was violated can be answered by asking if the warrant complies with Rule 41. See Levin, 2016 WL 2596010, at *3 (“The conduct underlying each of these alleged violations is identical: the magistrate judge’s issuance of a warrant to search property located outside of her judicial district. Moreover, because Section 636(a) expressly incorporates any authorities granted to magistrate judges by the Federal Rules of Criminal Procedure, the Court’s analyses of whether the NIT Warrant was statutorily permissible and whether it was allowed under Rule 41(b) are necessarily intertwined.” (citation omitted)); see also United States v. Matish, No. 4:16CR16, 2016 WL 3545776, at *16 (E.D. Va. June 23, 2016) (discussing Levin’s analysis of this issue).

The Court has already addressed Rule 41 and the good faith exception. See Anzalone I, 2016 WL 5339723, at *8-11. That analysis applies with equal force to the Federal Magistrates Act. Therefore, the Court concludes that the good faith exception applies even if issuance of the search warrant did not comply with Rule 41(b) and the Federal Magistrates Act.

C. Nature of Rule 41 Violation

The defendant contends that the government deliberately violated Rule 41, aware that the rule would not permit the NIT warrant issued in this case. As evidence, the defendant cites Special Agent Daniel Alfin's testimony from the hearing the Court held in Anzalone II. During that evidentiary hearing, Agent Alfin testified that the NIT warrant was vetted by the highest levels of the FBI and DOJ. See Docket No. 45, Ex. 5 at 46-47 (stating that the decision to seek the NIT warrant and continue operating Playpen "was done with the approval of executives in both the FBI and the Department of Justice"). As evidence of the DOJ's purported knowledge that Rule 41 did not permit the issuance of the NIT warrant, the defendant notes that DOJ recently sought amendments to Rule 41, changes which were recently enacted. See Fed. R. Crim. P. 41(b)(6)(A) ("[A] magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if . . . (A) the district where the media or information is located has been concealed through technological means."); see also 2016 Amendments to Fed. R. Crim. P. 41 advisory committee's note ("First, subparagraph (b)(6)(A) provides authority to issue a warrant to use remote

access within or outside that district when the district in which the media or information is located is not known because of the use of technology such as anonymizing software.").

A high-level vetting is evidence of good faith, not bad faith because the law is now clear as to whether Rule 41 would be violated in light of the novel nature of the technology. A number of courts have found that Rule 41 permitted the NIT warrant even before the 2016 amendments took effect. See, e.g., Matish, 2016 WL 3545776, at *17 (finding that Rule 41, as then written, authorized magistrate judge to issue the NIT warrant); United States v. Darby, No. 2:16CR36, 2016 WL 3189703, at *12 (E.D. Va. June 3, 2016) (same); United States v. Epich, No. 15-CR-163-PP, 2016 WL 953269, at *2 (E.D. Wis. Mar. 14, 2016) (same). The Court does not find that the government deliberately violated Rule 41.

D. Probable Cause

The defendant argues that there was no probable cause to issue the NIT warrant. The Court has already concluded otherwise. See Anzalone II, 2016 WL 5339723, at *6-7.

E. Franks Hearing

Only one new issue raised by the defendant gives the Court pause. The defendant requests a Franks hearing, asserting that Special Agent Daniel Alfin knew that the NIT warrant inaccurately described the images on the Playpen homepage and

that no probable cause would exist in the absence of this false portrayal. In a supplemental filing, the government asserts that Agent Alfin did not know that the homepage had changed before Special Agent Douglas Macfarlane submitted the search warrant application.

To obtain a Franks hearing, the defendant must make "a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit," and that the "allegedly false statement [was] necessary to the finding of probable cause." United States v. Castillo, 287 F.3d 21, 25 (1st Cir. 2002) (quoting Franks v. Delaware, 438 U.S. 154, 155–56 (1978)). "Suppression of the evidence seized is justified if, at such a hearing, the defendant proves intentional or reckless falsehood by preponderant evidence and the affidavit's creditworthy averments are insufficient to establish probable cause." United States v. Tanguay, 787 F.3d 44, 49 (1st Cir. 2015). "To prove reckless disregard for the truth, the defendant must prove that the affiant in fact entertained serious doubts as to the truth of the allegations." United States v. Ranney, 298 F.3d 74, 78 (1st Cir. 2002) (citation omitted).

There is no evidence that Agent Macfarlane personally knew of the updated homepage logo before submitting the warrant application. The application describes the Playpen site as it

appeared from September 16, 2014 to February 3, 2015. See Macfarlane Aff. ¶ 11, Docket No. 61, Ex. 1. On February 18, 2015, Agent Macfarlane learned that the site's URL had changed. See id. ¶ 11 n.3. That day, he accessed Playpen at the new URL "and determined that its content ha[d] not changed." Id.

The defendant maintains that Special Agent Daniel Alfin knew of the change before Agent Macfarlane submitted the search warrant application, and that Agent Alfin's knowledge should be imputed to the affiant for purposes of deciding whether to hold a Franks hearing. The Court agrees that, in some circumstances, a knowing or reckless omission by a fellow investigator may be grounds to hold a Franks hearing, even if the affiant himself did not know that his application contained material falsehoods or omissions. See United States v. DeLeon, 979 F.2d 761, 764 (9th Cir. 1992) ("A deliberate or reckless omission by a government official who is not the affiant can be the basis for a Franks suppression. The Fourth Amendment places restrictions and qualifications on the actions of the government generally, not merely on affiants.").

It is unclear, however, what Agent Alfin knew and when he knew it. The evidence the defendant cites regarding Agent Alfin's knowledge of the change to the homepage's appearance is based on testimony Agent Alfin gave in United States v. Jean, a Playpen case in the Western District of Arkansas. See Docket No.

45 at 21; Docket No. 45, Ex. 10. In that testimony, Agent Alfin explains that FBI agents began searching the home of Steven Chase, Playpen's principal administrator, on February 19, 2015. See Docket No. 45, Ex. 10 at 34-35. Sometime on February 19, Chase changed the logo from two prepubescent, partially clothed girls with their legs spread to one young girl wearing a short dress and black stockings with her legs crossed. That change was visible on Chase's laptop when the agents arrested him. In confusing testimony, Agent Alfin explains that he "did see the administrator's laptop screen. I did see that he was logged in to Playpen and so I did see the new logo." Id. at 35. Alfin, however, also states that he "did not observe the new logo at the time. It did not jump out to me as a significant or material change to the website." Id.

In supplemental briefing,[1] the government proffers that, although Agent Alfin "looked at the Playpen homepage on the early morning of February 20, 2015, prior to leaving the Chase residence, he did not notice that the image of two minor females had been replaced with an image of one minor female." Docket No. 68 at 3. "Only later did he learn that, just hours before law enforcement arrived at the Chase residence, the image of two

[1] The government states that it spoke with Special Agent Daniel Alfin about the homepage changes. See Docket No. 68 at 2. The government is ordered to submit an affidavit from Agent Alfin on this topic.

minor females was replaced with an image of one minor female." Id. "Special Agent Alfin stated that had he been aware of the change to the homepage prior to the submission of the Affidavit later on February 20, 2015, he would have taken steps to ensure that the description of the homepage in the Affidavit was updated to reflect the change." Id.

The Court does not decide whether Agent Alfin noticed the new logo or whether, if he had noticed it during the early morning hours of February 20, he was reckless in failing to relay that information to Agent Macfarlane before the search warrant application was submitted later that same morning. The Court need not address this issue because, even if Agent Alfin's conduct constituted recklessness, the new logo would not have changed the probable cause analysis. See Matish, 2016 WL 3545776, at *12 (holding that the "logo change lacks significance because the probable cause rested not solely on the site's logo but also on the affiant's description that the entire site was dedicated to child pornography, Playpen's suggestive name, the affirmative steps a user must take to locate Playpen, the site's repeated warnings and focus on anonymity, and the actual contents of the site"); Darby, 2016 WL 3189703, at *9 ("[C]ontrary to the repeated emphasis of Defendant, the images of two prepubescent females described in the warrant application were not necessary to the finding of

probable cause. There was an abundance of other evidence before the magistrate judge that supported her finding that there was probable cause to issue the warrant.").

The Court concludes that the defendant has not made the showing required for the Court to hold a Franks hearing.

ORDER

The defendant's motion to dismiss (Docket No. 44) and motion to suppress (Docket No. 45) are **DENIED**. The Court **ORDERS** the government to submit an affidavit from Special Agent Daniel Alfin regarding the content discussed in the government's December 15, 2016 proffer.

/s/ PATTI B. SARIS
Patti B. Saris
Chief United States District Judge